

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-46330

(43) 公開日 平成9年(1997)2月14日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A
G 0 6 F 13/00	3 5 1	9460-5E	G 0 6 F 13/00	3 5 1 G
G 0 9 C 1/00	6 3 0	7259-5J	G 0 9 C 1/00	6 3 0 A
		7259-5J		6 3 0 E
	6 6 0	7259-5J		6 6 0 E

審査請求 未請求 請求項の数3 O L (全 16 頁) 最終頁に続く

(21) 出願番号 特願平7-193447

(22) 出願日 平成7年(1995)7月28日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 室田 真男

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

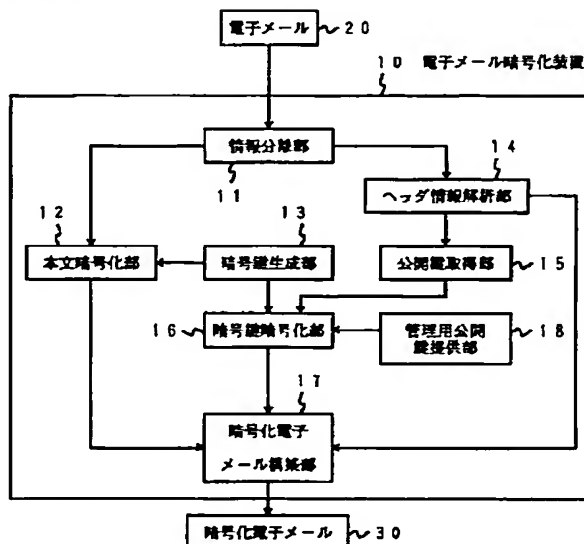
(74) 代理人 弁理士 鈴江 武彦

(54) 【発明の名称】 電子メール暗号化装置及び電子メール転送装置

(57) 【要約】

【課題】 電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる電子メール暗号化装置を提供すること。

【解決手段】 所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化する手段と、前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする。



【特許請求の範囲】

【請求項1】所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化する手段と、前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする電子メール暗号化装置。

【請求項2】電子メールの転送を行う電子メール転送装置において、転送対象とされた電子メールの種類を判別する手段と、判別された電子メールの種類に応じて該電子メールの転送の可否を判断する手段とを備えたことを特徴とする電子メール転送装置。

【請求項3】転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、この暗号化電子メールから該管理用の暗号鍵情報を取り除く手段をさらに備えたことを特徴とする請求項2に記載の電子メール転送装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子メール暗号化装置及び電子メール転送装置に関する。

【0002】

【従来の技術】コンピュータネットワークの普及に伴い、電子メールが広く利用されるようになってきた。さらには、秘匿すべき情報を電子メールとして転送したいという要求から、電子メール暗号化装置が提供されている。

【0003】暗号化電子メール装置は、PEM (Privacy Enhanced Mail) やPGP (Pretty Good Privacy) において実現されている。以下に、電子メールを暗号化する手順を示す。

【0004】まず、共通鍵暗号方式用の暗号鍵を生成し、その暗号鍵を用いて共通鍵暗号方式により電子メール本文を暗号化する。次に、本文の暗号化に用いた暗号鍵を、電子メールの送信者と受信者のそれぞれの公開鍵を用いて公開鍵暗号化方式により暗号化して、送信者用暗号鍵情報と受信者用暗号鍵情報を作成する。受信者が複数いる場合は、それぞれの受信者に対する暗号鍵情報を作る。そして、暗号化された本文と所定数の受信者用暗号鍵情報と送信者用暗号鍵情報が暗号化電子メールとして送られる。

【0005】このようにして暗号化された暗号化電子メールを受信者や送信者が読むときは、まず、自分用に付

与された暗号鍵情報を自分の秘密鍵を用いて復号して暗号鍵を得る。ここで用いる秘密鍵は、暗号鍵情報を作るときに用いられた公開鍵の対になっているものである。その秘密鍵を持っている者のみが、暗号鍵情報を復号して暗号鍵を得ることができる。暗号鍵を得た後は、共通鍵暗号方式を用いて本文を復号し読むことができる。

【0006】ところで、企業などにおいては、電子メールにより企業外部に秘密情報を漏洩されるのを防ぐために、電子メールの内容に関する情報管理を行ないたい要求がある。

【0007】本文が暗号化されていない電子メールの場合は、その内容は送信者と受信者以外でも読むことができるので、電子メール転送装置などにおいて電子メールのコピーをログとして保存することにより情報管理を行なうことができる。

【0008】ところが、従来の暗号化電子メールにおいて暗号化された本文を復号することができるのは、電子メールの送信者と受信者のみである。従って、電子メール転送装置において保存されたログを見ても、電子メール管理者は暗号化電子メールの内容を読むことができないため、情報管理をすることができないという問題点があった。

【0009】また、従来の電子メール転送装置は、電子メールの転送を要求されると、その電子メールのヘッダから受信者を読取って転送を行なうだけであった。従って、機密性の高い情報を持つ暗号化電子メールでも、要求があれば転送してしまうので、誤転送などのおそれがあり、セキュリティ上の大きな問題が残されていた。

【0010】

【発明が解決しようとする課題】従来の電子メール暗号化装置では、これにより暗号化された電子メールの内容を電子メールの管理者が読むことができないため、情報管理をすることができないという問題点があった。

【0011】また、従来の電子メール転送装置では、電子メールを無条件に転送していたので、セキュリティ上の問題点が残されていた。本発明は、上記事情に考慮してなされたものであり、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる電子メール暗号化装置を提供することを目的とする。また、本発明は、暗号化電子メールに関する転送制御を行うことができる電子メール転送装置を提供することを目的とする。

【0012】

【課題を解決するための手段】本発明（請求項1）は、所定の暗号鍵を用いて共通鍵暗号方式により暗号化した電子メールの本文に、該電子メールの送信者と受信者用の夫々の公開鍵を用いて公開鍵暗号方式により暗号化した該所定の暗号鍵を付加して暗号化電子メールを構築する電子メール暗号化装置において、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を

用いて前記所定の暗号鍵を暗号化する手段と、前記第三者の公開鍵により暗号化した前記所定の暗号鍵を前記電子メールに付加する手段とを備えたことを特徴とする。

【0013】本発明（請求項2）は、電子メールの転送を行う電子メール転送装置において、転送対象とされた電子メールの種類を判別する手段と、判別された電子メールの種類に応じて該電子メールの転送の可否を判断する手段とを備えたことを特徴とする。

【0014】本発明（請求項3）は、上記発明（請求項2）の電子メール転送装置において、転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、この暗号化電子メールから該管理用の暗号鍵情報を取り除く手段をさらに備えたことを特徴とする。

【0015】また、本発明に係る電子メール暗号化方法は、電子メールの本文を所定の暗号鍵を用いて共通鍵暗号方式により暗号化するステップと、該所定の暗号鍵を該電子メールの送信者用の公開鍵を用いて公開鍵暗号方式により暗号化するステップと、該所定の暗号鍵を該電子メールの受信者用の公開鍵を用いて公開鍵暗号方式により暗号化するステップと、予め定められた前記電子メールの受信者及び送信者以外の第三者の公開鍵を用いて前記所定の暗号鍵を暗号化するステップの4つのステップを所定の順番にあるいは並行して行なった後、暗号化された前記本文に前記夫々の公開鍵で暗号化された公開鍵を付加して暗号化電子メールを構築することを特徴とする。

【0016】また、本発明に係る電子メール転送方法は、転送対象とされた電子メールの種類を判別し、判別された電子メールの種類に応じて該電子メールの転送の可否を判断し、転送可能と判断された電子メールを転送することを特徴とする。

【0017】また、本発明に係る電子メール転送方法は、転送対象とされた電子メールの種類を判別し、判別された電子メールの種類に応じて該電子メールの転送の可否を判断し、転送可能と判断された電子メールが管理用の暗号鍵情報を含むものである場合、転送に先だってこの暗号化電子メールから該管理用の暗号鍵情報を取り除き、転送可能と判断された電子メールを転送することを特徴とする。

【0018】（作用）本発明（請求項1）では、電子メール暗号化装置が、電子メール本文の暗号化に用いた暗号鍵を電子メールの受信者と送信者以外の第三者の公開鍵により暗号化し、電子メールに付加する。その結果、本発明の電子メール暗号化装置により暗号化された電子メールは、受信者用、送信者用、第三者用のそれぞれの公開鍵で暗号化された暗号鍵情報が付けられる。したがって、この暗号化された電子メールを復号できるのは、受信者、送信者、そして第三者となる。ここで、第三者を電子メール情報管理者とすると、該管理者は電子メールの内容検査などの情報管理を行うことができる。

【0019】本発明（請求項2）では、入力された電子メールの種類を判別し、その結果に応じて該電子メールの転送の可否を判断する。例えば、電子メールが暗号化されていないものか、暗号化されたものかを判別する。さらには、暗号化電子メールについては、管理用暗号鍵情報を含むものであるか否かなど、種類をより細分化することもできる。そして、暗号化されていない電子メールだけ転送可、あるいは暗号化された電子メールについても、管理用暗号鍵情報を含む暗号化された電子メールは転送可、管理用暗号鍵情報を含まない暗号化された電子メールは転送不可、といったような判断を行う。そして、転送可能と判断された電子メールだけ転送する。

【0020】例えば、該電子メール転送装置を企業の内部と外部との境界に置くことにより、企業が情報管理できる電子メールのみを外部に転送する、といったことを行うことができる。

【0021】本発明（請求項3）では、上記発明（請求項2）の電子メール転送装置において、管理用の暗号鍵情報を含む暗号化電子メールから該暗号鍵情報を取り除く手段をさらに設けたので、メール送信者と受信者にとって本来不要である管理用の暗号鍵情報を除去することができる。

【0022】

【発明の実施の形態】以下、図面を参照しながらこの発明の実施の形態を説明する。図1に、本発明の第1の実施の形態に係る電子メール暗号化装置の基本構成を示す。電子メール暗号化装置10は、電子メール（図中20）を入力し、これを暗号化し、暗号化電子メール（図中30）として出力するものであり、情報分離部11、本文暗号化部12、暗号鍵生成部13、ヘッダ情報解析部14、公開鍵取得部15、暗号鍵暗号化部16、暗号化電子メール構築部17、管理用公開鍵提供部18を備えている。

【0023】図2は、暗号化の対象となる電子メールの基本的構造を示す。電子メール（20）は、ヘッダ情報部と本文（23）からなる。図2の例では、ヘッダ情報として送信者を表す送信者情報（21）と受信者を列記した受信者情報（22）が示されている。図2の例では、この電子メール（20）は送信者Sから受信者Aおよび受信者Bに宛てたものであることを示している。

【0024】図3には、電子メール暗号化装置10による電子メール暗号化処理の手順の一例を示す。以下、図3を参照しながら、電子メール暗号化処理を説明する。

【0025】電子メール暗号化装置10に入力された電子メール（20）は、情報分離部11により、送信者情報や受信者情報を含むヘッダ情報と本文に分けられる（ステップS1）。本文は本文暗号化部12に、ヘッダ情報はヘッダ情報解析部14に夫々送られる。

【0026】暗号鍵生成部13は、本文の暗号化に用いる共通鍵暗号方式の暗号鍵を生成する（ステップS

2)。生成された暗号鍵は、本文暗号化部12と暗号鍵暗号化部16に渡される。

【0027】本文暗号化部12は、該暗号鍵を用いて共通鍵暗号方式により本文を暗号化する(ステップS3)。共通鍵暗号方式としては、従来知られている方式、例えばDES(Data Encryption Standard)方式などを用いる。

【0028】暗号化された本文は、暗号化電子メール構築部17に渡される。ヘッダ情報解析部14は、ヘッダ情報の送信者情報(21)から送信者を、受信者情報(22)から受信者を解析する(ステップS4)。そして、この解析結果(図2の場合、送信者S/受信者A/受信者B)を公開鍵取得部15に渡す。また、ヘッダ情報は、暗号化電子メール構築部17に送られる。

【0029】公開鍵取得部15は、ヘッダ情報解析部14から送信者及び受信者の情報を渡されると、送信者及び受信者それぞれの公開鍵を取得する(ステップS5)。公開鍵の取得方法としては、例えば、ローカルにデータベースを持っていたりもよいし、公開鍵を提供するサーバからネットワーク経由で取得してきてもよい。取得された公開鍵は、暗号鍵暗号化部16に渡される。

【0030】管理用公開鍵提供部18は、電子メール管理用にあらかじめ定められた公開鍵を暗号鍵暗号化部16に渡す。管理用の公開鍵は、管理用公開鍵提供部18があらかじめ保有していてもよいし、別の場所から取得してきてもよい(ステップS7)。

【0031】ただし、入力電子メール(20)のヘッダ情報の受信者情報に管理者が書込まれていた場合には、上記のステップS5の処理で管理用公開鍵は入手されているので、管理用公開鍵提供部18から入手を省略してよい(ステップS6)。

【0032】暗号鍵暗号化部16は、暗号鍵生成部13で生成された前記暗号鍵を、公開鍵取得部15から受け取った受信者の公開鍵および送信者の公開鍵、ならびに管理用公開鍵提供部18から受け取った管理用の公開鍵を用いて、それぞれ公開鍵暗号方式により暗号化し、受信者用暗号鍵情報、送信者用暗号鍵情報、および管理用暗号鍵情報を作成する(ステップS8)。上記公開鍵暗号方式は、従来知られている方式、例えばRSA方式などを用いる。ここで生成された各暗号鍵情報は、暗号化電子メール構築部17に渡される。

【0033】暗号化電子メール構築部17は、本文暗号化部12より渡された暗号化された本文、暗号鍵暗号化部16より渡された受信者用暗号鍵情報、送信者用暗号鍵情報および管理用暗号鍵情報、ならびにヘッダ情報解析部14より渡されたヘッダ情報を用いて、暗号化電子メール(30)を構築して(ステップS9)、出力する。

【0034】図4は、図2の電子メール(20)を上記のようにして暗号化した暗号化電子メール(30)の構

造を示す。暗号化電子メール(30)は、送信者情報

(21)および受信者情報(22)からなるヘッダ情報、受信者A用暗号鍵情報(33)、受信者B用暗号鍵情報(34)、送信者S用暗号鍵情報(35)および管理用暗号鍵情報(36)からなる電子メール本文暗号鍵情報、ならびに暗号化本文(37)から構成される。

【0035】送信者情報(21)と受信者情報(22)は、図2の電子メールと同じもの(平文)である。受信者A用暗号鍵情報(33)には受信者Aの公開鍵、受信者B用暗号鍵情報(34)には受信者Bの公開鍵、送信者S用暗号鍵情報(35)には送信者Sの公開鍵、管理用暗号鍵情報(36)には管理用の公開鍵を用いて、それぞれ本文の暗号鍵が公開鍵暗号方式により暗号化された情報が記述されている。

【0036】電子メール受信者は、自分用の暗号鍵情報を自分が保有する秘密鍵により復号化して電子メール本文の暗号鍵を得ることができ、該暗号鍵を用いて電子メール本文を復号化することができる。ここで、各暗号鍵情報を復号して本文の暗号鍵を得ることができるのは、それぞれの公開鍵に対応する秘密鍵を保有する者だけである。

【0037】従って、図1の電子メール暗号化装置10により暗号化された暗号化電子メール(30)を復号して読むことができるのは、電子メール(20)の送信者、受信者A、受信者B、そして管理用の秘密鍵を有する管理者だけである。

【0038】この実施の形態の電子メール暗号化装置10による暗号化電子メール(30)は、送信者と受信者以外の第三者である管理者が電子メールを復号できる点に特徴がある。つまり、管理者により暗号化電子メール(30)の内容検査が可能となり、電子メールの情報管理が可能となる。従って、このような電子メール暗号化装置を、例えば、企業などによる電子メールの情報管理などに用いると効果的である。

【0039】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【0040】ところで、この実施の形態の電子メール暗号化装置の電子メール暗号化処理の手順は、図3に示したものに限らず、種々変形することができる。図5には、電子メール暗号化装置10による電子メール暗号化処理の手順の他の例を示す。図3の手順とは、処理の順番が異なっているだけである。すなわち、図3では、暗号化鍵を作成すると(ステップS2)、まず、電子メール本文の暗号化を行なったが(ステップS3)、図5では、電子メール本文の暗号化(ステップS22)は、暗号化電子メールフォーマットの構築の直前に行なっている(ステップS23)。また、図3では、送信者の判別と受信者の判別(ステップS4)をまとめて行ない、送

信者用公開鍵の取得と受信者用公開鍵の取得（ステップS5）をまとめて行ない、各公開鍵による本文の暗号鍵の暗号化（ステップS8）をまとめて行なっているが、図5では、まず、送信者について、判別（ステップS14）、送信者用公開鍵の取得（ステップS15）、公開鍵による本文の暗号鍵の暗号化（ステップS16）を行ない、次に、受信者について、判別（ステップS18）、送信者用公開鍵の取得（ステップS21）、公開鍵による本文の暗号鍵の暗号化（ステップS16）を行なっている。

【0041】また、これの他にも、種々の処理手順が考えられるが、当業者であれば容易に修正を施すことができるので、さらなる他の手順の例を一つ一つ説明することは省略する。

【0042】この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【0043】ここで、比較のために、図18に従来の電子メール暗号化装置の基本構成を示す。従来の電子メール暗号化装置がこの実施の形態と違う点は、管理用公開鍵提供部18を持たない点である。従って、暗号鍵暗号化部46は、電子メールの受信者と送信者の公開鍵のみを受け取り、受信者と送信者に対する暗号鍵情報のみを生成していた。

【0044】図19に、従来の電子メール暗号化装置による暗号化電子メールの構造を示す。図に示すように、暗号鍵情報としては受信者用暗号鍵情報（53、54）と送信者用暗号鍵情報（55）のみを含む。従って、該暗号化電子メールを読むことができるのは、送信者と受信者のみであり、第三者である管理者が電子メールの内容を検査するような情報管理を行うことができなかった。

【0045】次に、図6に、本発明の第2の実施の形態に係る電子メール暗号化装置の基本構成を示す。この電子メール暗号化装置60は、情報分離部61、本文暗号化部62、暗号鍵生成部63、管理用ヘッダ情報付加部64、ヘッダ情報解析部65、公開鍵取得部66、暗号鍵暗号化部67、暗号化電子メール構築部68を備えている。図6の管理用ヘッダ情報付加部64以外の部分は、基本的には、図1の対応する部分と同様のものである。つまり、図1の構成から管理用公開鍵提供部を省き、代りに管理用ヘッダ情報付加部を設けたものである。

【0046】また、図1に示す従来の電子メール暗号化装置との違いは、情報分離部61により分離されたヘッダ情報が、管理用ヘッダ情報付加部64に渡されその後ヘッダ情報解析部65に渡される点にある。

【0047】図7には、電子メール暗号化装置60によ

る電子メール暗号化処理の手順の一例を示す。以下、図7を参照しながら、電子メール暗号化処理を説明する。

【0048】電子メール暗号化装置60に入力された電子メール（20）は、情報分離部61により送信者情報や受信者情報を含むヘッダ情報と本文（23）に分けられる（ステップS21）。そして、本文は本文暗号化部62に、ヘッダ情報は管理用ヘッダ情報付加部64に夫々送られる。

【0049】暗号鍵生成部63は、本文の暗号化に用いる共通鍵暗号方式の暗号鍵を生成する（ステップS22）。生成された暗号鍵は、本文暗号化部62と暗号鍵暗号化部67に渡される。

【0050】本文暗号化部62は、該暗号鍵を用いて共通鍵暗号方式により本文を暗号化する（ステップS23）。暗号化された本文は、暗号化電子メール構築部68に渡される。

【0051】管理用ヘッダ情報付加部64は、電子メールの受信者情報にあらかじめ定められている電子メール管理者を加える（ステップS24）。つまり、電子メール（20）の受信者情報（22）には、受信者A、受信者B、管理者が載せられる。ヘッダ情報は、ヘッダ情報解析部65に渡される。

【0052】ヘッダ情報解析部65は、ヘッダ情報の送信者情報（21）から送信者を解析し、受信者情報から受信者を解析する（ステップS25）。そして、この解析の結果得られた送信者および受信者を公開鍵取得部66に渡す。この実施の形態では、受信者の中には、前記管理用ヘッダ情報付加部64で加えられた電子メール管理者が含まれる。なお、ヘッダ情報は、暗号化電子メール構築部68に送られる。

【0053】公開鍵取得部66は、送信者と受信者のそれぞれの公開鍵を取得する（ステップS26）。電子メール（20）の例では、送信者S、受信者A、受信者B、電子メール管理者の公開鍵を取得することになる。公開鍵の取得方法は、ここではとくに規定しない。取得した公開鍵は、暗号鍵暗号化部67に渡される。

【0054】暗号鍵暗号化部67は、暗号鍵生成部63で生成された前記暗号鍵を、公開鍵取得部66により渡された受信者の公開鍵、送信者の公開鍵、電子メール管理者の公開鍵を用いて、それぞれ公開鍵暗号方式により暗号化し、受信者用暗号鍵情報、送信者用暗号鍵情報、管理用暗号鍵情報を作成する（ステップS27）。ここで生成された各暗号鍵情報は、暗号化電子メール構築部68に渡される。

【0055】暗号化電子メール構築部68は、本文暗号化部62より渡された暗号化された本文、暗号鍵暗号化部67より渡された受信者用暗号鍵情報、送信者用暗号鍵情報、管理用暗号鍵情報、ヘッダ情報解析部65より渡されたヘッダ情報を用いて、暗号化電子メール（70）を構築して（ステップS28）、出力する。

【0056】図8は、図2の電子メール(20)を上記のようにして暗号化した暗号化電子メール(70)の構造を示す。暗号化電子メール(70)は、送信者情報(71)、受信者情報(72)からなるヘッダ情報、受信者A用暗号鍵情報(73)、受信者B用暗号鍵情報(74)、送信者S用暗号鍵情報(75)、管理用暗号鍵情報(76)からなる電子メール本文暗号鍵情報、そして暗号化本文(77)からなる。

【0057】このように、この実施の形態による暗号化電子メールにも、管理用暗号鍵情報が付加されるので、第1の実施の形態と同様、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる。

【0058】さらに、図8の暗号化電子メール(70)は、図4の暗号化電子メール(30)と相違し、受信者情報に暗号化電子メール管理者が加えられている。こうすることにより、電子メール管理者用の暗号鍵情報がつけられる。また、電子メールが電子メール管理者にも配送されることになり、暗号化電子メールのログ機能を自動的に行うこともできる。

【0059】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【0060】ところで、この実施の形態の電子メール暗号化装置の電子メール暗号化処理の手順は、図7に示したものに限らず、種々変形することができる。図9には、電子メール暗号化装置60による電子メール暗号化処理の手順の他の例を示す。図7の手順とは、処理の順番が異なっているだけである。すなわち、図7では、暗号化鍵を作成すると(ステップS22)、まず、電子メール本文の暗号化を行なったが(ステップS23)、図9では、電子メール本文の暗号化(ステップS41)は、暗号化電子メールフォーマットの構築の直前に行なっている(ステップS42)。また、図7では、送信者の判別と受信者の判別(ステップS25)をまとめて行ない、送信者用公開鍵の取得と受信者用公開鍵の取得(ステップS26)をまとめて行ない、各公開鍵による本文の暗号鍵の暗号化(ステップS27)をまとめて行なっているが、図9では、まず、送信者について、判別(ステップS35)、送信者用公開鍵の取得(ステップS36)、公開鍵による本文の暗号鍵の暗号化(ステップS37)を行ない、次に、受信者について、判別(ステップS39)、送信者用公開鍵の取得(ステップS40)、公開鍵による本文の暗号鍵の暗号化(ステップS37)を行なっている。

【0061】また、これの他にも、種々の処理手順が考えられるが、当業者であれば容易に修正を施すことができるので、さらなる他の手順の例を一つ一つ説明することは省略する。

【0062】この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【0063】次に、図10に、本発明の第3の実施の形態に係る電子メール暗号化装置の基本構成を示す。この電子メール暗号化装置80は、情報分離部81、本文暗号化部82、暗号鍵生成部83、管理用ヘッダ情報付加部84、ヘッダ情報解析部85、公開鍵取得部86、暗号鍵暗号化部87、暗号化電子メール構築部88を備えている。図10の各部分は、基本的には、図6の対応する部分と同様のものである。ただし、この実施の形態では、第2の実施の形態と異なり、情報分離部81で分離したヘッダ情報を暗号化電子メール構築部88に与えている。

【0064】また、図18に示す従来の電子メール暗号化装置との違いは、情報分離部81により分離されたヘッダ情報が、管理用ヘッダ情報付加部84と暗号化電子メール構築部88に渡される点である。

【0065】この実施の形態の電子メール暗号化装置80による電子メール暗号化処理の手順は、基本的には、図7や図9と同様である。もちろん、前述した実施の形態と同様に、図7や図9に示したものに限らず、種々変形することができる。

【0066】この実施の形態が第2の実施の形態と異なるのは、情報分離部81で分離したヘッダ情報を暗号化電子メール構築部88に与えているので、ヘッダ情報解析部85に渡される電子メールの受信者情報には電子メール管理者は含まれるが、暗号化電子メール構築部88に渡される電子メール受信者情報には電子メール管理者は含まれない点にある。

【0067】従って、この実施の形態によれば、図4と同様の暗号化電子メールを構築することができる。もちろん、この実施の形態による暗号化電子メールにも、管理用暗号鍵情報が付加されるので、第1、第2の実施の形態と同様、電子メールの送信者及び受信者以外の第三者が暗号化電子メールに関する情報管理を行うことができる。

【0068】また、この実施の形態によれば、従来の暗号化電子メールの枠組を大きく変えることなく第三者による暗号化電子メールの情報管理を行うことができるという利点がある。

【0069】もちろん、この実施の形態の電子メール暗号化装置は、ハードウェアで実現することも可能であり、また、上記のような処理内容に相当するプログラムを作成し、これをコンピュータにインストールして実行させる形で実現することも可能である。

【0070】なお、第2の実施の形態で暗号化電子メールを構築する際に、ヘッダ情報の受信者情報から管理者

を削除するようにしても、図 4 と同様の暗号化電子メールを構築することができる。

【0071】次に、図 11 に、本発明の第 4 の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、暗号化電子メールの転送を制限する機能を有するものである。この電子メール転送装置 90 は、暗号化電子メール判別部 91、電子メール転送判断部 92、電子メール転送部 93 を備えている。

【0072】暗号化電子メールの転送の制限には、種々のものが考えられる。例えば、

①暗号化電子メールはすべて転送不可能とする。

②所定の条件を満たす暗号化電子メールのみ転送可能とする。例えば、暗号化電子メールの転送可能者リストを保有し、送信者がそのリストに載っているときのみ転送可能とする。

【0073】図 12 には、上記①の転送制限をする場合の転送処理手順の一例を示す。電子メール転送装置 90 に入力された電子メールは、暗号化電子メール判別部 91 により該電子メールが暗号化電子メールであるかどうか判別される（ステップ S51）。その方法は様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。暗号化電子メール判別部 91 は、その結果を電子メール転送判断部 92 に送る。

【0074】電子メール転送判断部 92 は、暗号化電子メール判別部 91 の結果を基に該電子メールが転送可能かどうかの判断を行う。ここでは、暗号化電子メールでなければ転送可能とし（ステップ S52）、暗号化電子メールの場合は転送不可とする（ステップ S54）。

【0075】転送可能と判断されたメールは、電子メール転送部 93 に送られて転送される（ステップ S53）。電子メール転送部 93 は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【0076】図 13 には、上記②の転送制限をする場合の転送処理手順の一例を示す。電子メール転送装置 90 に入力された電子メールは、暗号化電子メール判別部 91 により該電子メールが暗号化電子メールであるかどうか判別される（ステップ S61）。その方法は様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。暗号化電子メール判別部 91 は、その結果を電子メール転送判断部 92 に送る。

【0077】電子メール転送判断部 92 は、暗号化電子メール判別部 91 の結果を基に該電子メールが転送可能かどうかの判断を行う。ここでは、暗号化電子メールの

転送可能者リストを保有しているものとする。

【0078】暗号化電子メールの場合は、転送可能とする（ステップ S61）。暗号化電子メールの場合は、電子メールのヘッダ情報の送信者情報を参照し、送信者がその転送可能者リストに載っている場合、転送可能とし（ステップ S64、S62）、載っていない場合、転送不可とする（ステップ S64、S65）。

【0079】転送可能と判断されたメールは、電子メール転送部 93 に送られて転送される（ステップ S63）。暗号化電子メールの転送の制限には、上記以外にも種々のものが考えられる。

【0080】このように、この実施の形態によれば、暗号化電子メールに関する転送制御を行うことができる。次に、図 14 に、本発明の第 5 の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、管理者用暗号鍵情報を含む暗号化電子メールは転送し、管理用暗号鍵情報を含まない暗号化電子メールは転送しない機能を有するものである。この電子メール転送装置 100 は、暗号化電子メール判別部 101、電子メール転送判断部 102、電子メール転送部 103、管理用暗号鍵情報検査部 104 を備えている。

【0081】図 15 には、この実施の形態の転送処理手順の一例を示す。電子メール転送装置 100 に入力された電子メールは、暗号化電子メール判別部 101 により該電子メールが暗号化電子メールであるかどうか判別される（ステップ S71）。その方法は、第 4 の実施の形態と同様、様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。

【0082】その結果が、暗号化電子メールである場合は、管理用暗号鍵情報検査部 104 により、該暗号化電子メールが管理用の暗号鍵情報を正しく含んでいるかどうかの検査を行う（ステップ S74）。その方法は様々であるが、例えば、暗号化電子メール内に管理用暗号鍵情報が含まれているかどうかを走査することにより検査することができる。また、管理用暗号鍵情報を含む暗号化電子メールのヘッダ情報に特別の識別子を含むようにしておけば、そのヘッダ情報を含むかどうかを検査する方法もある。

【0083】暗号化電子メール判別部 101 は、管理用暗号鍵情報検査部 104 の出力を受け、その結果を電子メール転送判断部 102 に送る。電子メール転送判断部 102 は、暗号化電子メール判別部 101 の結果を基に、該電子メールが転送可能かどうかの判断を行う。暗号化電子メールでなければ転送可能とし（ステップ S72）、暗号化電子メールの場合は、管理用の暗号鍵情報を含んでいる暗号化電子メールの場合は転送を行い（ステップ S74、S72）、含んでいない暗号化電子メー

ルの場合は転送を行わない(ステップS74、S75)。

【0084】転送可能と判断されたメールは、電子メール転送部103に送られて転送される(ステップS73)。電子メール転送部103は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【0085】この実施の形態で述べた電子メール転送装置を、例えば、企業と外部との境界に設けることにより、管理用の暗号鍵情報を含まない暗号化電子メール、つまり電子メール管理者が情報管理を行うことができない暗号化電子メールを企業の外に出ないように設定することができる。

【0086】次に、図16に、本発明の第6の実施の形態に係る電子メール転送装置を示す。この電子メール転送装置は、管理用の暗号鍵情報を消去する機能を有するものである。この電子メール転送装置110は、暗号化電子メール判別部111、電子メール転送判断部112、電子メール転送部113、管理用暗号鍵情報検査部114、管理用暗号鍵情報除去部115を備えている。

【0087】図17には、この実施の形態の転送処理手順の一例を示す。電子メール転送装置110に入力された電子メールは、暗号化電子メール判別部111により該電子メールが暗号化電子メールであるかどうか判別される(ステップS81)。その方法は、第4の実施の形態と同様、様々であるが、例えば、暗号化電子メールの場合は、ヘッダ情報あるいは本文の一部に暗号化電子メールであることを示す情報が含まれるので、それが含まれるかどうかを検索することにより暗号化電子メールの判別を行う。

【0088】その結果が、暗号化電子メールである場合は、管理用暗号鍵情報検査部114により、該暗号化電子メールが管理用の暗号鍵情報を正しく含んでいるかどうかの検査を行う(ステップS84)。その方法は、前述の第5の実施の形態と同様とする。暗号化電子メール判別部111は、管理用暗号鍵情報検査部114の出力を受け、その結果を電子メール転送判断部112に送る。

【0089】電子メール転送判断部112は、暗号化電子メール判別部111の結果を基に、該電子メールが転送可能かどうかの判断を行う。該電子メールが暗号化電子メールでなければ転送可能とし(ステップS82)、電子メール転送部113に送る。該電子メールが暗号化電子メールの場合は、管理用暗号鍵情報を含んでいない場合は転送不可とし(ステップS84、S85)、管理用暗号鍵情報を含んでいる場合は転送可能とする(ステップS84、S87)。転送可能と判断された暗号化電子メールは、管理用暗号鍵情報除去部115に送られる。

【0090】管理用暗号鍵情報除去部115は、電子メ

ール転送判断部112から送られてきた暗号化電子メールから管理用暗号鍵情報を取り除き(ステップS86)、電子メール転送部113に送る。

【0091】転送可能と判断されたメールは、電子メール転送部113に送られて転送される(ステップS83)。電子メール転送部113は、公知の電子メール転送方式と同様の機能を有し、ここでは機能の説明を省略する。

【0092】この実施の形態により、第1～第3の実施の形態(図1、図6、図10)の電子メール暗号化装置にて付加された管理用暗号鍵情報を暗号化電子メールから取り除くことができる。管理用暗号鍵情報は、ある組織内の情報管理にのみ必要なものであり、送信者と受信者にとっては、本来不必要な情報である。したがって、この実施の形態の電子メール転送装置を用いることにより、余分な管理用の情報を削除することができる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0093】

【発明の効果】本発明(請求項1)によれば、電子メール本文の暗号化に用いた暗号鍵を電子メールの受信者と送信者以外の第三者の公開鍵により暗号化し、電子メールに付加するので、当該暗号化電子メールを受信者および送信者以外のもので第三者も復号することができる。

【0094】従って、第三者の公開鍵を電子メール情報管理者用のものにすれば、該管理者は電子メールの内容検査などの情報管理を行うことができる。本発明(請求項2)によれば、入力された電子メールの種類を判別し、その結果に応じて該電子メールの転送の可否を判断するので、電子メールの種類に応じた電子メールの転送の可否を判断基準を適宜設定することにより、電子メールの転送制御を行なうことができる。

【0095】本発明(請求項3)によれば、上記発明(請求項2)の電子メール転送装置において、管理用の暗号鍵情報を含む暗号化電子メールから該暗号鍵情報を取り除く手段をさらに設けたので、メール送信者と受信者にとって本来不要である管理用の暗号鍵情報を除去することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る電子メール暗号化装置の基本構成を示す図

【図2】電子メールの基本的構造を示す図

【図3】同実施の形態の電子メール暗号化処理の手順の一例を示すフローチャート

【図4】同実施の形態に係る電子メール暗号化装置から出力される暗号化電子メールの構造を示す図

【図5】同実施の形態の電子メール暗号化処理の手順の他の例を示すフローチャート

【図6】本発明の第2の実施の形態に係る電子メール暗

号化装置の基本構成を示す図

【図 7】同実施の形態の電子メール暗号化処理の手順の一例を示すフローチャート

【図 8】同実施の形態に係る電子メール暗号化装置から出力される暗号化電子メールの構造を示す図

【図 9】同実施の形態の電子メール暗号化処理の手順の他の例を示すフローチャート

【図 10】本発明の第 3 の実施の形態に係る電子メール暗号化装置の基本構成を示す図

【図 11】同第 4 の実施の形態に係る電子メール転送装置の基本構成を示す図

【図 12】同実施の形態の転送処理手順の一例を示すフローチャート

【図 13】同実施の形態の転送処理手順の他の例を示すフローチャート

【図 14】同第 5 の実施の形態に係る電子メール転送装置の基本構成を示す図

【図 15】同実施の形態の転送処理手順の一例を示すフローチャート

【図 16】同第 6 の実施の形態に係る電子メール転送装

置の基本構成を示す図

【図 17】同実施の形態の転送処理手順の一例を示すフローチャート

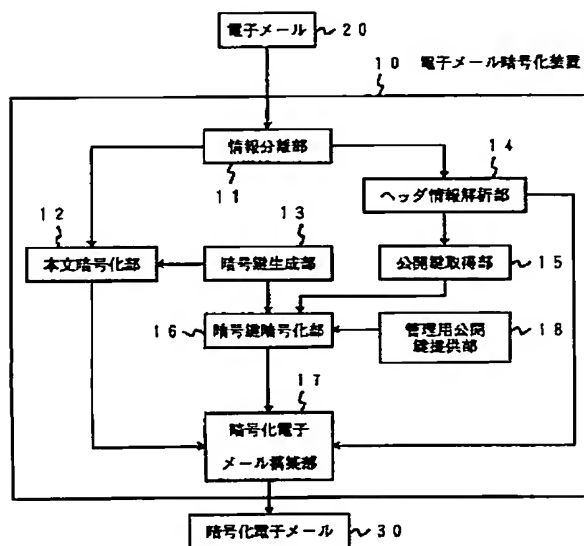
【図 18】従来の電子メール暗号化装置の基本構成を示す図

【図 19】従来の電子メール暗号化装置による暗号化電子メールの構造を示す図

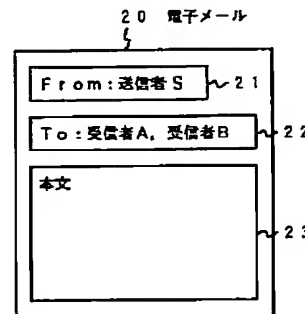
【符号の説明】

10, 60, 80…電子メール暗号化装置、11, 61, 81…情報分離部、12, 62, 82…本文暗号化部、13, 63, 83…暗号鍵生成部、64, 84…管理用ヘッダ情報付加部、14, 65, 85…ヘッダ情報解析部、15, 66, 86…公開鍵取得部、16, 67, 87…暗号鍵暗号化部、17, 68, 88…暗号化電子メール構築部、18…管理用公開鍵提供部、90, 100, 110…電子メール転送装置、91, 101, 111…暗号化電子メール判別部、92, 102, 112…電子メール転送判断部、93, 103, 113…電子メール転送部、104, 114…管理用暗号鍵情報検査部、115…管理用暗号鍵情報除去部

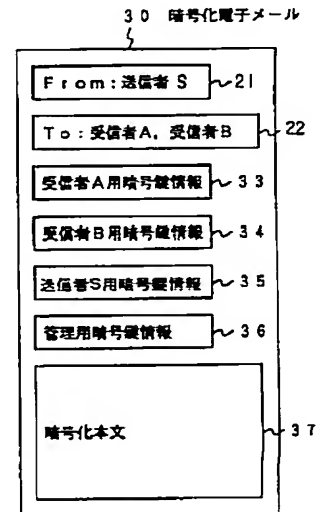
【図 1】



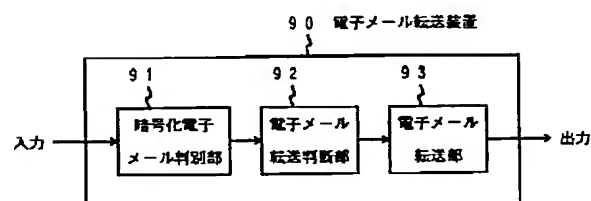
【図 2】



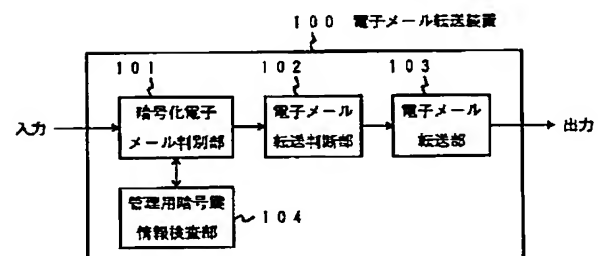
【図 4】



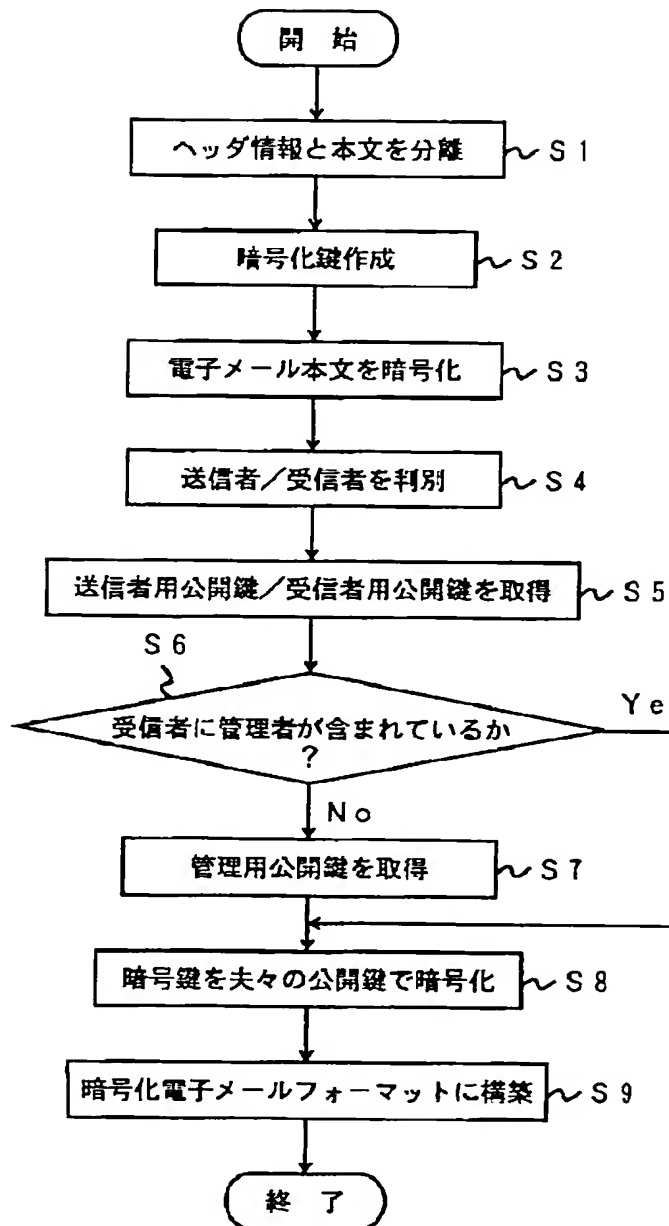
【図 11】



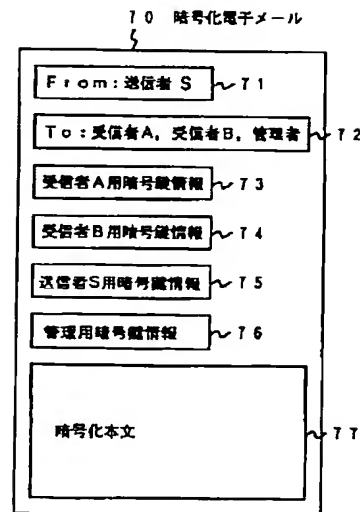
【図 14】



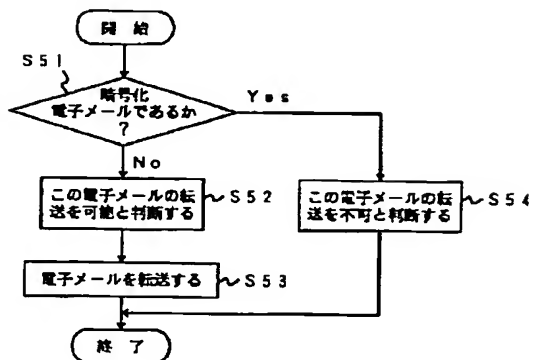
【図3】



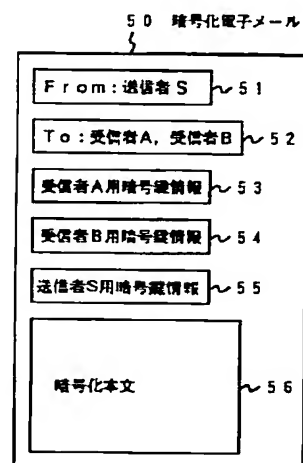
【図8】



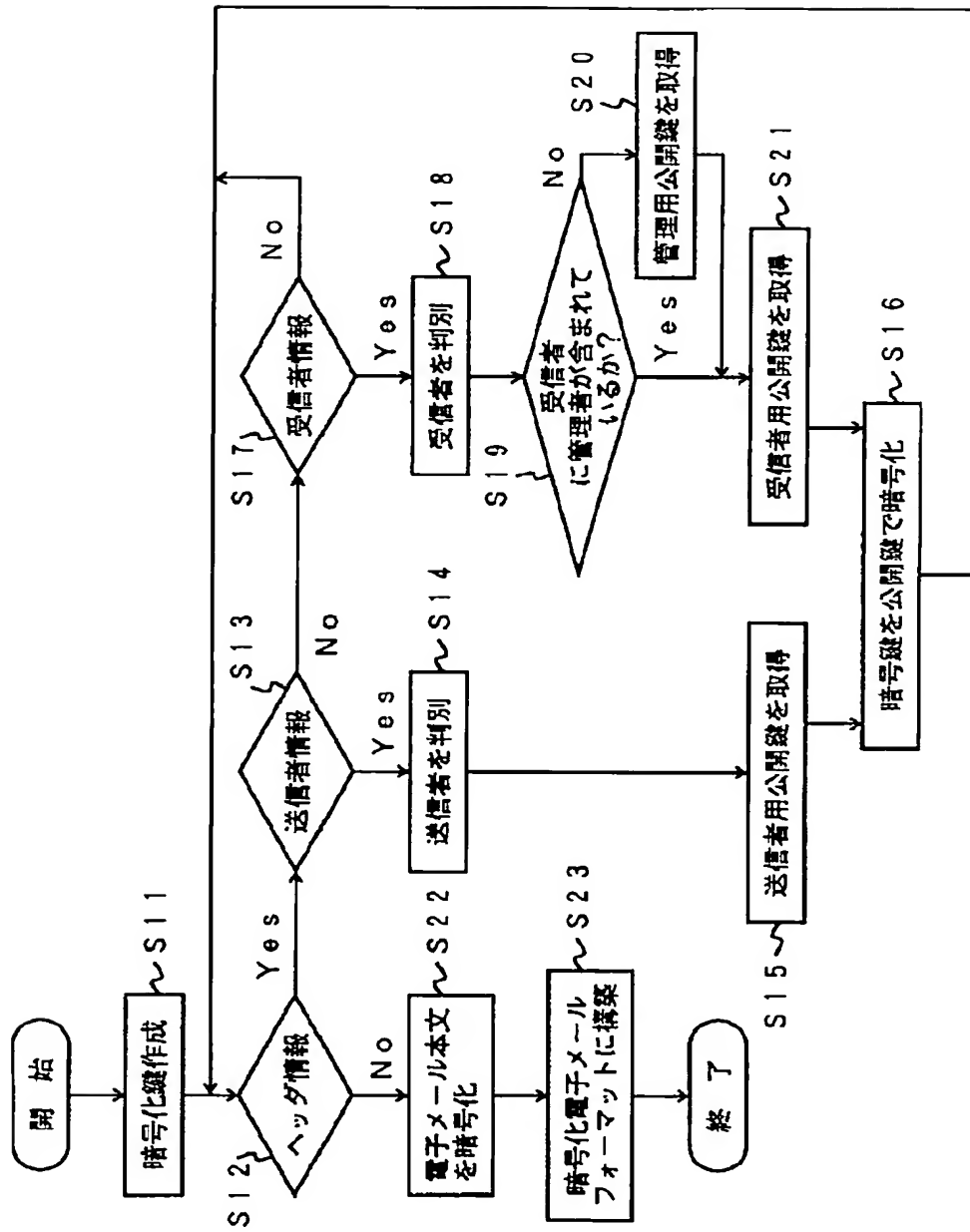
【図12】



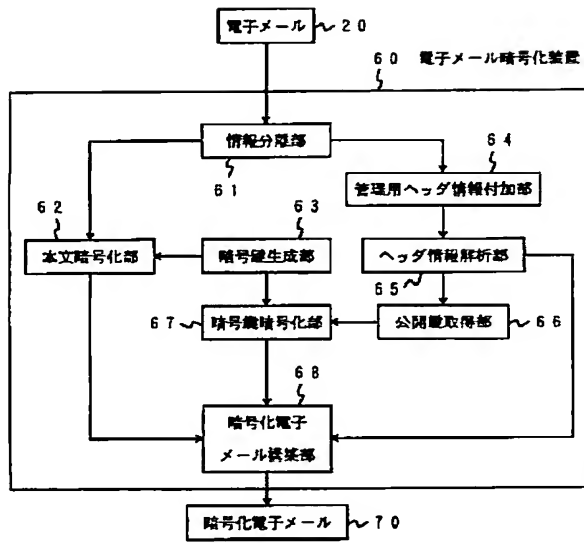
【図19】



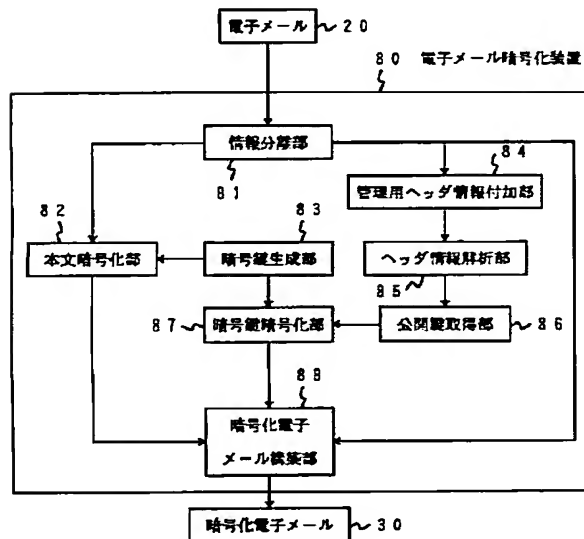
【図5】



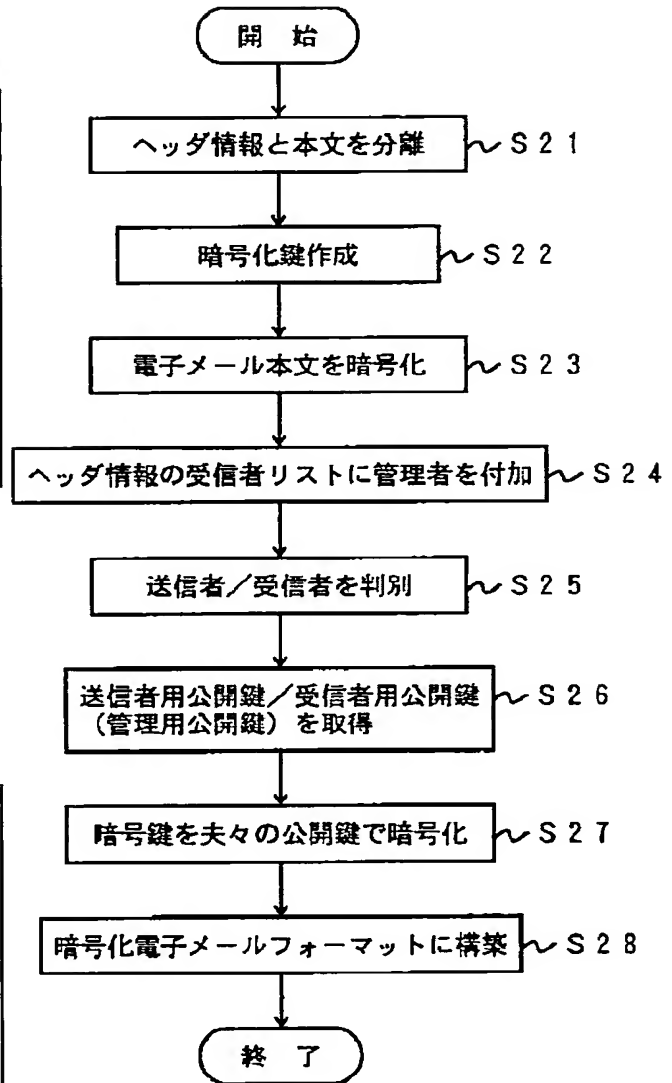
【図6】



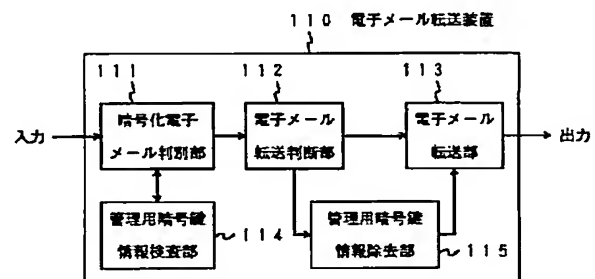
【図10】



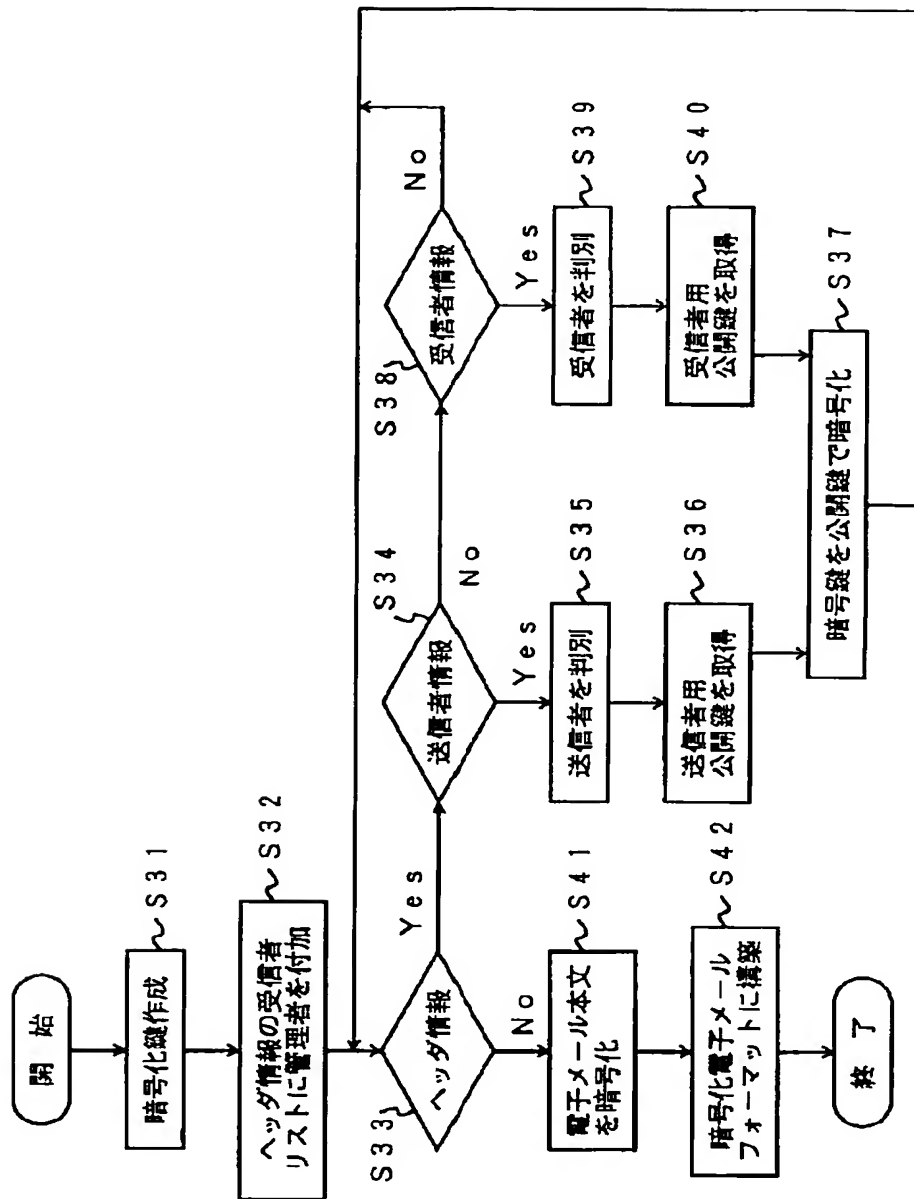
【図7】



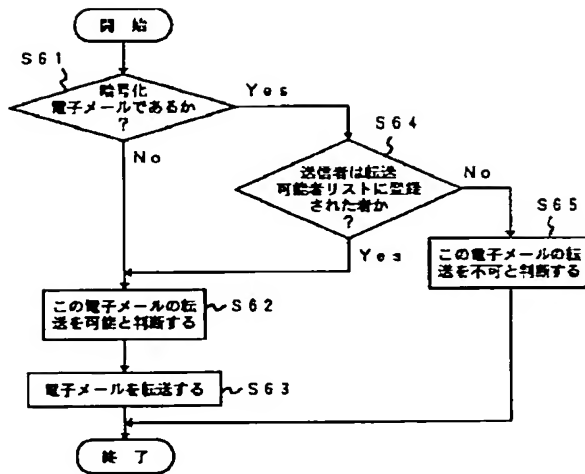
【図16】



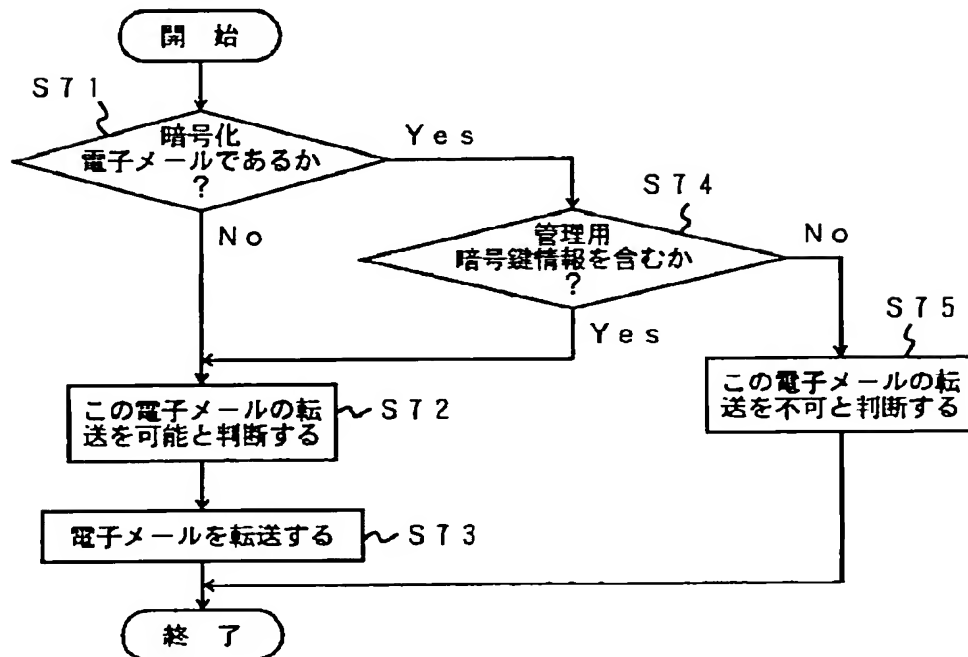
【図9】



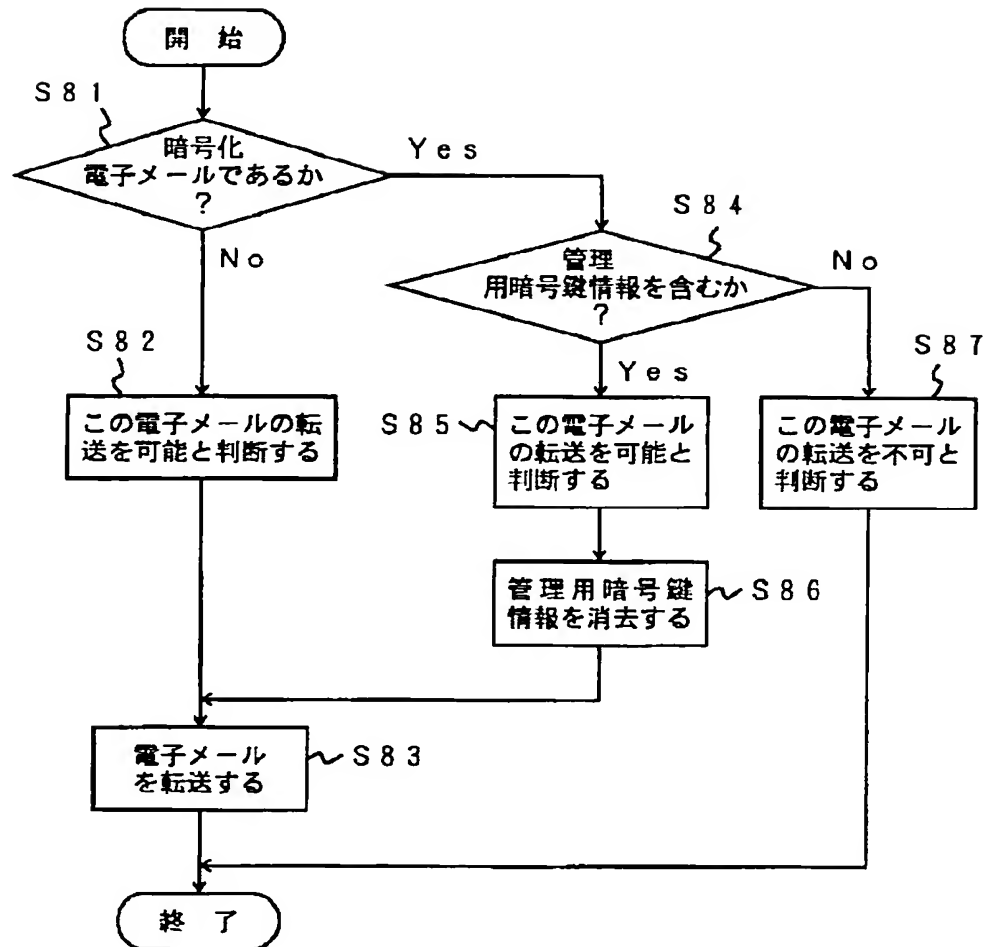
【図13】



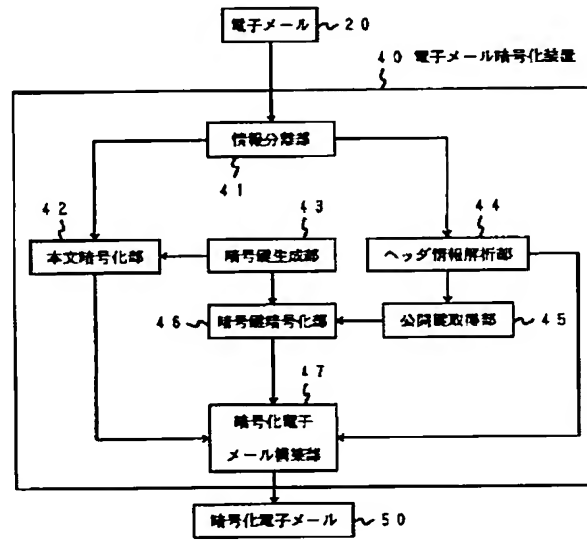
【図15】



【図17】



【図 1 8】



フロントページの続き

(51) Int. Cl.⁶

H 0 4 L 12/54

12/58

識別記号

庁内整理番号

F I

H 0 4 L 9/00

11/20

技術表示箇所

6 0 1 E

1 0 1 B

9466-5K